CLAIMS

We claim:

1. A method for blocking unsolicited e-mail being transmitted to an e-mail server at an Internet Service Provider (ISP) from a remote server when a roaming customer of the ISP logs onto the Internet through the remote server, comprising:

receiving a user identification (USERID) and a password associated with the roaming customer;

retrieving a plurality of data associated with the roaming customer from a Authentication, Authorization, and Accounting (AAA) database located at the ISP based on the USERID and password;

authenticating the remote customer using the retrieved plurality of data;

assigning an IP address to the remote customer;

dynamically adding the IP address to a plurality of valid IP address associated with the ISP;

logging onto a mail server at the ISP from the remote server using the IP address and the plurality of data used to authenticate the roaming customer at the remote server, wherein only the remote customer may accesses the mail server using the assigned IP address from the remote server.

2. The method of claim 1, wherein authenticating the roaming customer comprises:

transmitting the USERID and password associated with the roaming customer to an authentication server at the ISP;

comparing the USERID and password against each USERID and password associated with every registered user of the ISP;

generating a negative response if the USERID and password associated with the roaming customer does not match a USERID and password associated with any of the registered customers;

generating a positive response if the USERID and password associated with the roaming customer matches a USERID and password associated with at least one of the registered customers; and

generating a START record, the START record indicating the beginning of the roaming customer's access to the mail server.

3. The method of claim 1, wherein the plurality of IP address associated with the ISP are used only by roaming customers registered with the ISP to access the Internet through the remote server.

4. The method of claim 1, wherein dynamically adding the roaming customer's IP address to a pool of valid IP address comprises:

reading the START record, timestamp, RELAY from the AAA database; and

forwarding the START record, USERID, password, and IP address to the mail server for adding the IP address to the pool of valid IP addresses.

5. The method of claim 1, wherein logging onto the mail server comprises:

initiating an SMTP request to send e-mail from an e-mail application server; and

validating the IP address of the roaming customer against the pool of valid IP addresses.

6. The method of claim 1, further comprising logging off the roaming customer from the remote server.

7. The method of claim 6, wherein logging off the roaming customer, comprises:

generating a termination signal by the roaming customer;

transmitting the roaming customer's USERID to the remote network to identify the roaming customer to be logged off;

transferring the USERID to the Authentication server on the ISP;

generating STOP record and transferring the STOP record to the AAA Server ISP, wherein the STOP record is operable to identify the roaming customer.

8. The method of claim 7, wherein generating the STOP record is further operable for determining whether the roaming customer has sent any unauthorized email messages.

9. A method of connecting a roaming customer to a foreign network access server to prevent unsolicited e-mails from being transmitted from the foreign network access server (NAS) to the roaming customer's Internet Service Provider (ISP), comprising:

receiving a user command through an Internet device associated with the roaming customer to connect to the foreign NAS;

transmitting a user identification (USERID) and a password from the Internet device to the foreign NAS, wherein the USERID and password are associated with the roaming customer;

transmitting the USERID, password to an Authentication, Authorization, and Accounting AAA Server located at the roaming customer's ISP for the purpose of authenticating the roaming customer as a registered user of the ISP;

generating a positive response if the roaming customer is a registered user of the ISP;

assigning a local IP address to the roaming customer, the local IP address being selected from a plurality of IP address at the foreign NAS;

generating a START record indicating that the roaming customer is being logged onto the system;

writing the START record to a database located at the roaming customer's ISP.

10. The method of claim 9, further comprising generating a negative response if the roaming customer is not a registered user at the ISP.

11. The method of claim 10, wherein generating a negative response comprises not allowing the roaming customer to authenticate, and denying the roaming user access to the Internet through the NAS.

12. The method of claim 9, wherein the START record comprises a NAS IP address, a NAS protocol, a NAS port type, a User name, a called ID station, a calling station ID, an account status type, an account authentication, a service type, an account session ID, a framed protocol, an account delay time, and a start timestamp.

13. The method of claim 9, wherein the AAA database contains data organized similar to a Terminal Access Controller Access Control System (TACACS) format.

14. The method of claim 13, wherein the AAA database has been modified to include a USERID field.

15. A method of logging on a roaming customer onto a mail server located at the roaming customer's Internet Service Provider (ISP) via a foreign network access server (NAS) while preventing the unauthorized distribution of foreign SPAM messages from the NAS to the mail server, comprising:

establish a network connection between the NAS and the ISP;

authenticating that the roaming customer is a registered customer of the ISP;

storing a data log in a database at the ISP, the data log comprising a plurality of attributes to track the roaming customers usage of the network connection;

transferring the data log to a mail access server at the ISP;

assigning an IP address to the roaming customer to access the mail server;

adding the IP address assigned to the roaming customer to a list of a valid IP address from the NAS that are allowed to access the mail server on the ISP; and

connecting the roaming user to the mail server using the IP address from the NAS.

16. The method of claim 15, further comprising removing the IP address from the list of valid IP address upon receiving a command to log off the roaming customer from mail server.

17. The method of claim 15, wherein authenticating the roaming customer comprises:

receiving a user identification (USERID) and a password associated with the roaming customer;

transferring the USERID and password to an authentication server at the ISP;

comparing the USERID and password from the roaming customer to a list USERIDs and passwords associated with each registered customers of the ISP stored at the authentication server;

transmitting a positive response to the NAS if the USERID and password associated with the roaming customer matches a USERID and password associated with a registered customer from the list stored at the authentication server; and

transmitting a negative response to the NAS if the USERID and password does not match a USERID and password associated with at least one registered customer of the ISP from the list stored at the authentication server.

18. The method of claim 15, further comprising, creating a data log associated with the roaming customer at the time the roaming customer logs onto the mail server, wherein the data log comprises a START identifier, the USERID and password associated with the roaming customer, the IP address assigned to the roaming customer, a RELAY to the mail server from the NAS and a timestamp indicating the starting time the roaming customer logged onto the mail server.